CH-4 entered 24 Jun 98
CH-3 entered 2 Apr 97
CH-2 entered 6 Jan 97
CH-1 entered 11 Jul 95
NAVSUBSCOLINST 5510.3F
O1E
1 Apr 94

NAVSUBSCOL INSTRUCTION 5510.3F

Subj: COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) OPNAVINST 5510.1H
(b) OPNAVINST 5239.1A
(c) OPNAVINST 5530.14B
(d) DOD C-5105.21-M-1
(e) NWP-0
(f) Manual of the Judge Advocate General
(g) OPNAVINST 5513.1D
(h) SUBASENLONINST 2300.3H
(I) SECNAVINST 5720.42E
(j) NAVSUBSCOLINST 5530.2D
(k) DOD 5220.22M
(l) SECNAVINST 5212.5C
(m) NAVSUBSCOLINST 5239.3A

Encl: (1) Naval Submarine School Information and Personnel Security Manual

1. Purpose. To update procedures for implementation of the command information and personnel security program in support of broader direction contained in references (a) through (m).

2. Cancellation. NAVSUBSCOLINST 5510.3E. This instruction has been revised extensively and should be read in its entirety.

3. Applicability. The provisions of this instruction apply to all military and civilian personnel attached to Naval Submarine School.

4. Information. Enclosure (1) contains specific security procedures to identify responsibilities for the command information and personnel security program. It is meant as a supplement to reference (a) and they must be used in conjunction with each other. Repetition of those parts of reference (a) which do not require specific guidance, or are not applicable to this command, have been avoided. Where discrepancy may exist, reference (a) takes precedence over enclosure (1).

W. A. PETERS

Distribution:
Case A

NAVAL SUBMARINE SCHOOL
INFORMATION AND PERSONNEL SECURITY MANUAL

TABLE OF CONTENTS

PART I - PROGRAM MANAGEMENT

1-1 Security Organization

1. Department Head, Security Department. The Commanding Officer is ultimately responsible for effective management of the Security Program at Naval Submarine School. The Department Head is responsible to the Commanding Officer in all matters associated with security and to the Executive Officer for all administrative matters. The Department Head also will be assigned as the Security Officer.

2. Command Security Manager. To administer the Information and Personnel program daily, a Command Security Manager will be appointed in writing by the Commanding Officer and will serve as the principal advisor on all security matters outlined in reference (a). The Command Security Manager will report directly to the Department Head, Security Department for all administrative matters and to the Commanding Officer for issues of command security concern. A complete listing of all areas of responsibility can be found in Articles 2-7 and 2-8 of reference (a) and on pages A5-1and A5-2 of this instruction.

3. Assistant Command Security Manager. The Assistant Command Security Manager will be the division officer of the Classified Material Control Center (CMCC) and is delegated visit approval authority for the command. The Assistant Command Security Manager will be responsible specifically for the following:

a. Ensuring compliance with accounting and control requirements for material classified Secret or Confidential, including receipt, distribution, inventory, reproduction and disposition.

b. Ensuring control of visits to and from the command when the visitor is authorized access to classified information.

c. Ensuring all personnel who handle classified information or are assigned to sensitive duties are cleared appropriately and requests for personnel security investigations are prepared, submitted and monitored properly.

d. Ensuring personnel security investigations, clearances, and access are recorded.

4. Department Security Assistant. Due to the large and multi-building nature of this command, each department will designate a Department Security Assistant, E-6 or above, with the background and experience to manage the department's program successfully. These personnel will be listed in NAVSUBSCOLNOTE 5420. Personnel acting as Department Security Assistants must have at least a Secret security clearance. Department Security Assistant responsibilities include, but are not limited to the following:

a. Serving as primary liaison between their department and the Command Security Manager on matters pertaining to the security of classified information and personnel security.

b. Developing and maintaining the department emergency action plan using the guidelines provided in paragraph 2-16 of reference (a) and paragraph 1-2 of this instruction.

c. Immediately notifying the Command Security Manager/ Physical Security Officer upon discovery of all threats to security, compromises or other violations occurring within their department.

d. Administering and documenting the Department security education program. This program will consist of orientation briefings, refresher briefings, on-the-job training, counter-espionage briefings, debriefings, and any special briefings, debriefings, and any special briefings as required.

e. Coordinating with the Command Physical Security Assistants and Department Information Security Officer on matters of common concern.

f. Maintain department security instructions.

g. Maintain all forms for posting on security containers, doors, telephones, reproduction machines, and telecopiers (fax machines).

h. Track department security deficiencies and corrective actions. Inform the Security Manager and Physical Security Officer of changes in status.

* NOTE: Although the size and complexity of Naval Submarine School demands delegation, the Command Security Manager is still responsible for the Information and Personnel Security Program for the command as a whole, and will provide the guidance, coordination and oversight necessary to ensure the program is being administered effectively.

5. Department Classified Material Custodians. Each department will designate a Department Classified Material Custodian and Alternate, E-5 or above, with the background and experience to manage the department's classified material inventory. These personnel will be listed in NAVSUBSCOLNOTE 5420, and will have a letter of designation on file in the CMCC. The Department Material Custodians will:

a. Report directly to the CMCC and Security Manager regarding compliance with accounting and control requirements for material classified Secret and Confidential held by the department.

b. Ensure all classified material is safeguarded in accordance with reference (a) of this instruction.

c. Distribute and maintain a record of all material classified Secret in the custody of the sub-custodian within the department.

d. Check with the CMCC daily to determine if there is classified material for their department. All Secret material should be picked up within **one** working day after being placed on accountability.

e. Conduct monthly Secret audits and refer discrepancies to the CMCC for resolution. Twice annually when directed by the CMCC, conduct a sight inventory of all pieces of material signed out to the department.

f. Upon relief of duties as Department Custodian, conduct a sight inventory of all material in that department and report the results to the CMCC. Department Sub-custodians must also conduct a sight inventory of material signed out to them and report the results to the Department Custodian. Any discrepancies in audits or inventory must be reported to the CMCC.

g. Report any discrepancies concerning the department's Information and Personnel Security Program to the Department Security Assistant.

6. Top Secret Control Officer (TSCO). The Top Secret Control Officer will be appointed in writing and is responsible to the Command Security Manager for the receipt, custody, accounting for, and disposition of Top Secret material at Naval Submarine School. Specific responsibilities are outlined in paragraph 2-10 of reference (a).

7. Automated Information System Security Officer (AISSO). The AISSO will be assigned by the command as directed by reference (b). The AISSO is responsible to the Department Head, Security Department for the protection of classified information being processed on automated information systems and responsible to the Security Officer for the protection of the equipment and related resources per reference (m).

8. Internal Security Officer (ISO). The ISO is responsible to the Security Officer, Executive Officer, and Commanding Officer on all matters pertaining to internal security of the command and loss prevention including, but not limited to, the following:

a. Coordinates all internal security investigations.

b. Maintains security instructions.

c. Oversees security badge program.

d. Serves as Key and Lock Officer.

e. Strong room certification/decertification.

f. Responsible for annual surveys, random inspections, and periodic monitors.

g. Perform security briefs/debriefs.

h. Conducts Command security training (GMT).

9. Internal Security Assistant (ISA). The ISA is responsible to the ISO on all matters pertaining to internal security of the command including, but not limited to, the following:

a. Responsible for Security Badge Program.

b. Serves as command locksmith.

c. Strong room certification/decertification.

d. Performs annual surveys, random inspections, and periodic monitoring.

e. Conducts security briefs/debriefs."

10. Special Security Officer (SSO). Naval Submarine School is accredited for and authorized to receive, process and store Sensitive Compartmented Information (SCI). The SSO is responsible for the security, control and utilization of SCI, as well as for the operation of the Sensitive Compartmented Information Facility (SCIF). Guidelines for this program are provided in reference (d). The SSO may be designated as Command Security Manager but the Command Security Manager cannot function as the SSO unless specifically approved by Commanding Officer of Naval Intelligence.

11. Naval Warfare Publications Library Custodian. The Naval Warfare Publications Library Custodian (NWPLC) will be assigned as required by reference (e).

1-2 Emergency Plans

1. Each department which handles classified information will adhere to the emergency plan outlined in Appendix (1). This plan provides for the protection of classified material in case of fire, natural disaster/severe weather, civil disturbance, and acts of terrorism including bomb threats. This plan is as detailed as possible but specific procedures and responsibilities must be assigned by departments which handle classified material.

2. Each department will be responsible for ensuring staff and students are educated in the procedures to follow during an emergency. The Command Security Manager will review the command plan at least annually and update as necessary.

1-3 Security Education Program

1. Basic Policy. Regardless of position, rank or grade, as personnel assigned to Naval Submarine School should be familiar with command policies and procedures. The purpose of the command security education program is to ensure all personnel are aware of the need, and the procedures, for safeguarding classified information.

2. Indoctrination. All staff personnel arriving at Naval Submarine School will attend the command indoctrination course. During the course they will receive a briefing on the command security organization, an overview of the Information and Personnel Security Program, and an Operations Security briefing.

3. Orientation. Those personnel who are assigned to a billet or course of instruction requiring access to classified material also will receive a security orientation briefing and sign a statement of acknowledgement given them by the Department Security Assistant. Appendix (2) will be used for this purpose. The Department Security Assistant will retain this acknowledgement as long as the member is attached to Naval Submarine School. If a course of instruction will expose students to Naval Nuclear Propulsion Information, the Supplemental Security Statement (Appendix (3)) also will be executed.

4. On-the-Job Training. On-the-job training is that aspect of the security education program when application of specific security procedures is learned. Supervisors are responsible for conducting and monitoring on-the-job training with subordinate personnel.

5. Refresher Briefings. All personnel who have access to classified information must receive an annual refresher briefing designed to enhance security awareness. This briefing will be conducted annually using guidance provided by the Command Security Manager. Documentation of attendance by command personnel will be maintained in department security education and/or training files.

6. Counterespionage Briefings. Every two years those who have access to material classified Secret or above must be given a counterespionage briefing by a Naval Criminal Investigative Service (NCIS) agent. Department Security Assistants are responsible for scheduling these briefings and maintaining a roster of personnel required to attend. The Department Security

Assistant will forward a report of completed training with names of personnel who attended each briefing.

7. Debriefings

a. The Security Termination Statement (OPNAV 5511/14) will be executed prior to termination of active military/civilian service, upon expiration of a Limited Access Authorization (LAA), when a security clearance is revoked for cause, and when a security clearance is administratively withdrawn. The Assistant Command Security Manager is responsible for conducting this briefing and for ensuring that the original OPNAV 5511/14 is placed in the individual's official personnel record for permanent retention or, if executed at the end of an LAA, is retained for two years in command files.

b. Upon transfer, either inter-departmental or to another command, personnel will receive a security debriefing and sign the Security Debriefing Acknowledgment contained in Appendix (4). Department Security Assistants will conduct this briefing prior to signing the member's check out sheet, and will maintain the signed debriefing acknowledgment for two years.

c. Students graduating or disenrolled for any reason from course of instruction also shall execute the Security Debriefing Acknowledgment. The Department Security Assist will maintain records of these debriefings for two years.

1-4 Security Violations and Compromises

1. Security Violations. There are two types of security violations. One results in the loss, compromise or possible compromise of classified information. The other involves a failure to adhere to security regulations but does not result in a loss, compromise, or possible compromise.

2. Compromise. Compromise is the disclosure of classified information to a person who is not authorized access and is confirmed when conclusive evidence exists that the disclosure has occurred. A possible compromise occurs when conclusive evidence exists that classified information has been subjected to unauthorized disclosure or when classified information was not stored or controlled properly.

3. Sanctions. Reference (a) details the administrative sanctions, punitive actions, and non-punitive ramifications for personnel who knowingly or willfully violate the provision of that regulation concerning the protection of classified information. To ensure compliance with reference (a), security violations, compromises and possible compromises of any type will be investigated vigorously and prevented from recurring by correcting the problems causing the violation.

4. Initial Action. Any individual who becomes aware of a compromise or possible compromise of classified material will immediately notify the Command Quarterdeck, who will notify the Command Duty Officer, Command Security Manager and the Department Director concerned. The Command Security Manager will notify the Executive Officer and will contact Naval Criminal Investigative Service (NCIS) Regional Investigative Officer New London. If NCIS assumes responsibility for the investigation, evidence will be preserved and the command Preliminary Inquiry (PI) will be postponed, pending NCIS permission to continue.

5. Preliminary Inquiry

a. When classified information has been lost, compromised or subjected to compromise, a preliminary inquiry (PI) will be conducted after notification has been made to NCIS by the Command Security Manager. The inquiry will be completed within seventy-two hours using Exhibits 4A and 4B of reference (a) as a guide. This is not a Manual of the Judge Advocate General (JAGMAN) investigation. The goal at this point is to determine whether a compromise or loss has occurred, the nature of the information involved and potential for damage to national security.

b. Upon completion of the PI, the investigator will forward the final report to the Commanding Officer, via the Command Security Manager, Legal Officer, and the Executive Officer. The report will be in narrative format and will contain the pertinent data required by paragraph 4-4 of reference (a). If the PI report determines that compromise or loss cannot be ruled out, a letter or message, depending on the level of threat involved, will be sent to the addressees listed in Exhibit 4B of reference (a) for a determination of further action.

c. PI investigators will be E-7 or above, assigned by the CMAA. The investigator must hold a clearance that will at least match the level of classification of the material involved.

*Note: It should be emphasized that a PI is not a JAGMAN investigation and does not require the depth of report mandated for a JAGMAN.

6. JAG Manual Investigation

a. A determination of loss or compromise by the PI will result in referral of the incident to the Legal Officer for possible assignment of a JAGMAN investigation. All JAGMAN investigations will be conducted using guidelines of references (a) and (f).

b. Results will be forwarded by endorsement up the chain of command to CNO (N92) with a copy provided to Naval Criminal Investigative Service Regional Office New London.

7. Other Security Violations

a. Violations of security regulations not resulting in compromise or loss will be dealt with at the command level. These violations will be prosecuted vigorously and disciplinary action may be required. In addition, reevaluation of eligibility for access to classified information may be necessary for those responsible for the security violation.

b. Other security violations include, but are not limited to, improper handling of classified material, improper courier procedures, discussion of classified information over unsecured telephone lines, or failure to secure classified material properly.

8. Unsecured Containers. If a container holding classified material is found unlocked in the absence of assigned personnel, the Command Duty Officer (CDO) will be informed immediately, and the container will be guarded until the CDO arrives. The CDO will inspect the classified material involved. If possible compromise of the material has occurred, the CDO will recall the custodian of that safe to conduct a complete inventory of its contents. If the CDO does not believe that a possible compromise has occurred, he/she will secure the container and report the security violation to the Executive Officer and the Command Security Manager the next working day.

1-5 Counterintelligence Matter to be Reported to the Naval Criminal Investigative Service (NCIS)

1. Basic Policy. Chapter 5 of reference (a) gives detailed information concerning counterintelligence matters that may require NCIS action and must be reported. The following list of activities must be reported immediately to the Command Security Manager or directly to NCIS Regional Office New London.

a. Contact with any individual, regardless of nationality, whether within or outside the scope of the individual's official activities, in which:

(1) Illegal or unauthorized access is sought to classified or otherwise sensitive information; or

(2) The employee is concerned that he or she may be the target of exploitation by a foreign entity.

b. Any facts or circumstances of a reported contact with any individual that appear to:

(1) Indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive or classified information or technology; or

(2) Offer a reasonable potential for such; or

(3) Indicate the possibility of continued contact with the individual for such purposes.

c. If anyone having access to classified information either attempts or commits suicide, all available information will be sent to NCIS. NCIS must be an addressee in all messages dealing with suicide or attempted suicide.

2. Unauthorized Absences

a. The Command Legal Office will provide the names of all staff and student personnel deemed to be in an unauthorized absentee (UA) status. The possibility of compromise or loss of classified information will be examined by the department to which the member belonged and a memorandum reporting the results of that determination will be forwarded to the Command Security Manager **IMMEDIATELY**.

b. Staff members who are reported UA and are responsible for classified information (Department Security Assistants, Classified Material Custodians, etc.) will be considered to be security risks and reported to NCIS. Departments will be required to initiate and conduct a complete inventory of all classified material within their possession or cognizance within 24 hours, regardless of the day of the week.

APPENDIX 1

EMERGENCY ACTION PLAN FOR THE PROTECTION OF CLASSIFIED MATERIAL

1. Purpose. The purpose of this plan is to provide guidance and outline procedures for the protection of classified material in the event of an emergency.

2. Scope. This appendix directs action to be taken to protect classified information in the event of fire, natural disaster/severe weather, civil disturbance, or acts of terrorism (including bomb threats). This guidance provides for the protection of classified material in a way that will minimize risk of loss of life or injury to personnel.

3. Preparation

a. In order to prepare for the protection of classified material in the event of any emergency, department directors and Classified Material Custodians must ensure that classified holdings are kept to an absolute minimum. Specifically, duplicate copies of classified material, outdated material, and should be destroyed properly.

b. All security containers must be marked with a number or symbol on the exterior, indicating priority in the event of emergency evacuation. The external marking will not indicate the level of classified information stored in the container. All NAVSUBSCOL security containers will be marked as outlined below. Whenever practicable, the number shall be placed in white on the front of the container and any previous markings should be removed or marked out.

(1) Those containing the most sensitive material (Top Secret) will be marked with the number “3".

(2) Those containing Secret material will be marked with the number “2".

(3) Those containing the least sensitive material (Confidential) will be marked with the number “1".

4. Key Personnel. Only certain personnel can declare an emergency condition leading to the evacuation of classified material. The Commanding Officer, Executive Officer, Department Heads, the Command Security Manager, and the Command Duty Officer each have the authority to declare an emergency situation.

5. Procedures. Personnel safety shall be of paramount concern. In the case of immediate danger due to fire or other disaster, the first priority will be evacuation of the building involved. In other emergency situations, the procedures outlined below will be executed to the extent possible.

a. Emergency Evacuation

(1) In the event of an emergency evacuation of any office, classroom, training space, or building containing classified material, the supervisor in charge of the affected area if responsible for the safeguarding of classified material.

(2) If time permits, every attempt will be made to place classified material in authorized storage containers (including certified strongrooms). The lock should be secured by rotating the dial four times in the same direction. However, it is not necessary to obtain a second check or to fill out the SF 702.

(3) Each department will assign personnel as Control Point Access Watches (CPAW) at entrances/exits of affected areas. The CPAW will ensure only emergency personnel are permitted access.

(4) Following an evacuation, all hands shall muster at a point designated by their department head.

(5) When re-entry to the building or space is authorized, an inventory of all classified material which was left unsecured will be conducted using the inventory list provided by the Classified Material Control Center (CMCC).

(6) If an emergency occurs after normal working hours, it is the responsibility of the Duty Petty Officer to ensure the building is evacuated and a CPAW is posted.

b. Fire and Natural Disaster

(1) Upon sounding of the fire alarm, personnel will evacuate the area immediately. If time permits, personnel shall secure classified material as described in paragraph 5.a. above

(2) Due to the construction of NAVSUBSCOL buildings, any natural disaster likely to occur in this area will probably not cause a breach of security. However, if the Commanding Officer, Command Security Manager, or Command Duty Officer deems the nature of the disaster sufficient to warrant concern over the protection of classified material, evacuation will be conducted as described in paragraph 5.e. below.

c. Civil Disturbance

(1) Because NAVSUBSCOL building are located within the confines of Naval Submarine Base, New London, the likelihood of a breach of security for classified material due to civil disturbance is very low.

(2) If a civil disturbance is reported, all classified material will be stored in approved security containers and will remain in storage until resolution of the disturbance.

d. Bomb Threat/Terrorist Action

(1) Upon notification of a bomb threat, personnel will immediately evacuate the area. The department head involved will determine, based on the authenticity of the threat, whether or not to secure classified material prior to evacuation.

(2) If the department head determines that classified material should not be secured due to imminent danger, the Department Director will assign a CPAW at all entrances/exits to assist in controlling access. The CPAW will not be posted as to put his/her safety at risk.

(3) When re-entry to the building or space is authorized, an inventory will be conducted using the inventory list provided by the Classified Material Control Center (CMCC).

e. Emergency Evacuation

(1) Should an emergency threaten a specific building or space, evacuation of the classified material within that area may become necessary if time permits.

(2) If directed by anyone of the key personnel listed in paragraph 4, classified material in danger will be relocated to an area predetermined by the department head. If the area is not available, it is the responsibility of the Command Duty Officer to designate an alternate storage site.

(3) When evacuating material, every effort will be made to maintain positive accountability. Material placed in its designated evacuation area will be segregated from other classified material as much as possible.

(4) Upon completion of the evacuation, an inventory will be conducted by the division involved and a report to the CMCC made outlining what was moved and to what location.

6. Additional Guidance. Procedures for the protection of SCI material in an emergency situation are contained in NAVSUBSCOLINST 5501.6B. Procedures for the protection of Communications Security Material (CMS) are contained in NAVSUBSCOLINST 2250.2G.

APPENDIX 2

SECURITY ORIENTATION AND STATEMENT OF ACKNOWLEDGEMENT

As a minimum, the following areas will be discussed with new personnel as part of initial check-in. This is intended as a minimum guide; each department must ensure that all security related information is fully covered during this brief.

1. **COMMAND SECURITY ORGANIZATION**

Command Security Manager

Assistant Security Manager

Department Security Manager

2. **SPECIFIC COMMAND SECURITY PRECAUTIONS**

Classification of material to which access is granted

Storage requirements

Areas of physical security

Special security precautions: (Badge system, etc.)

3. **INDIVIDUAL SECURITY RESPONSIBILITIES**

Classified information will not be discussed in a non-secure area, over a telephone, or in any way that would allow access by an unauthorized person.

Any information concerning terrorist threat against U.S. assets must be reported.

Any attempt by an unauthorized person to acquire classified information must be reported.

Any contact with an individual which suggests the member may be the target of exploitation by a foreign intelligence agency must be reported (i.e. offers of money, bribes, promises or threats to family members under foreign control, extravagant gifts, etc.)

Any information which could reflect on the trustworthiness of an individual who has access to classified information must be reported.

PUNISHMENTS FOR UNAUTHORIZED DISCLOSURE/LOSS OF CLASSIFIED MATERIAL per United States Code Title 18 are as follows:

Section 793 - Gathering, transmitting, or losing Defense information: $10,000 and/or 10 years.

Section 794 - Gathering or delivery of Defense information to aid foreign governments: Death or up to life imprisonment.

Section 795 - Photographing and sketching Defense installations: $1,000 and/or 1 year

Section 796 - Use of aircraft for photographing Defense installations: $1,000 and/or 1 year

Section 797 - Publication and sale of photographs of Defense installations: $1,000 and/or 1 year

Section 798 - Disclosure of classified information: $10,000 and/or 10 years

Violations of United States Code, Title 18, Sections 793, 794, and 798 are considered felonies and, upon conviction, individuals are ineligible to hold any office, or place of honor, profit, or trust berated by the Constitution or laws of the United States.

NAVAL NUCLEAR PROPULSION PROGRAM SECURITY INDOCTRINATION STATEMENT

(Member initials here if this statement applies; insert N/A if not applicable) I certify that I have received an oral security indoctrination concerning the special restrictions governing the handling, stowage, disposal, and control of US Naval Nuclear Propulsion Information as defined in CG-RN-1 Rev 1, ERDA-DOD Classification Guide for Naval Nuclear Propulsion Program.

I CERTIFY THAT I FULLY UNDERSTAND MY RESPONSIBILITIES CONCERNING THE SAFEGUARDING OF CLASSIFIED INFORMATION.

(Printed name)	(Signature)
(Witness signature)	(Date)

STATEMENT OF ACKNOWLEDGEMENT
CONTINUATION SHEET

Continuation sheet for Orientation/Debriefing (circle one)

COURSE _____ CLASS _____

PRINTED NAME (LAST, FIRST, MI)	SIGNATURE
WITNESS:	
INSTRUCTOR	DATE

APPENDIX 3

NAVAL NUCLEAR PROPULSION PROGRAM SUPPLEMENTAL SECURITY STATEMENT

Commanding Officer
Naval Submarine School
Box 700, Groton, CT 06349-5700

1. I, _____, have been informed and am aware of special controls with respect to the disclosure of US Naval Nuclear Propulsion Information*, both classified and unclassified, as defined below. Specifically, I have read and understand that:

a. No US Naval Nuclear Propulsion Information, classified or unclassified, may be disclosed to any foreign national or foreign government except under an approved government-to-government agreement, executed in accordance with the Atomic Energy Act of 1954, as amended; such disclosures are authorized only through specially designated official channels.

b. It is the policy of the United States Government not to participate in and not to authorize United States firms or individuals to participate in foreign naval nuclear propulsion plant projects, except for an Agreement for Cooperation on naval nuclear propulsion executed in accordance with Section 123d of the Atomic Energy Act of 1954, as amended.

c. Validated export license must be obtained from the Office of Export Control, US Department of Commerce, before a US firm or individual may disclose any technology in connection with a foreign maritime (i.e., non-military) nuclear propulsion plant project.

2. I HEREBY CERTIFY THAT I am not retaining nor taking away with me from my place of employment (duty) any documents or things containing or incorporating naval nuclear propulsion information, classified or unclassified.

3. I will not hereafter in any manner reveal or divulge to any person, except as specifically authorized by the United States Government, any US Naval nuclear propulsion information, classified or unclassified.

*US Naval Nuclear Propulsion Information is defined as all information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance and repair of the propulsion plants of naval nuclear powered ships, including the associated nuclear support facilities.

Signature	Signature of Witness
Rank/Rate, SSN	Type or Print Name of Witness
Date	Title of Witness

Continuation sheet attached: Yes No

APPENDIX 4

SECURITY DEBRIEFING ACKNOWLEDGEMENT

By my signature, I certify my understanding and compliance with the following:

1. All classified material to which I have had access has been returned to its proper stowage place and/or custodian.

2. I have no classified material in my possession.

3. I shall not communicate or transmit classified information orally or in writing to any unauthorized person or agency. I understand that the burden is upon me to determine whether or not information is classified and to agree to obtain the decision of the Chief of Naval Operations or his authorized representative on such matters prior to disclosing information which is or may be classified.

4. I will report to the Naval Criminal Investigative Service (or to FBI or nearest DOD Component if no longer affiliated with the Department of the Navy), without delay, any incident of an attempt by an unauthorized person to solicit classified information.

5. I have been informed and am aware that Title 18 U.S.C., Sections 793-799, as amended, and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I have been informed and am aware that the making of a willfully false statement herein renders me subject to trial as provided by Title 18 U.S.C. 1001.

_____(Initial if Naval Nuclear Propulsion Supplemental Security Statement has been included as part of this debriefing.)

_____	_____
(Printed name)	(Signature)
_____	_____
(Witness)	(Date)

APPENDIX 5

COMMAND SECURITY MANAGER/SECURITY OFFICER

a. Basic Function. The Security Manager/Security Officer is responsible for all security matters, to include information resource management, physical security, and information and personnel security.

b. Duties, Responsibilities, and Authority:

(1) Identify areas in which improved physical security and loss prevention measures are required and provide recommendations for such improvements to the Commanding Officer.

(2) Serve as the Commanding Officer's advisor and direct representative regarding security of classified information.

(3) Develop, prepare, and maintain a current command Physical Security Plan in accordance with OPNAVINST 5530.14 (series).

(4) Develop written command security procedures including a Unit Emergency Plan. Emergency Destruction Bills are integrated with the Unit Emergency Plan.

(5) Develop, prepare, and maintain physical security instructions which address required physical security procedures.

(6) Supervise accounting and control of classified material including receipt, distribution, inventory, reproduction and disposition procedures.

(7) Establish personnel identification and access control systems.

(8) Ensure all personnel who handle classified information hold the appropriate level of security clearance based on a need to know and that all requests for personnel security investigations are prepared, submitted and monitored properly.

(9) Conduct annual physical security surveys.

(10) Provide technical assistance to the Commanding Officer on physical security matters and adequate security training for all personnel within the command.

(11) Coordinate physical security requirements with host commands and ensure such requirements are set forth in appropriate host-tenant, inter-service support, or licensing agreements.

(12) Ensure clearance status and unit access grants are recorded and accessible for verification.

(13) Coordinate preparation of classification guides and development of security planning within the command.

(14) Coordinate and ensure security control over visits to and from the command.

(15) Ensure security violations and compromises are reported, recorded, and investigated vigorously.

(16) Oversee the command Key and Lock Control Program.

(17) Participate in planning, directing, coordinating and implementing procedures for crisis management of situations (including hostage situations) which pose a threat to the physical security of the command, and provide adequate advice to the Commanding Officer during crisis which relate to physical security.

(18) Establish and maintain liaison and working relationships and agreements Federal Investigative agencies, local Naval Criminal Investigative Service components, state and local law enforcement and fire protection authorities.

(19) Serve as facilitator and be responsible for records of the Command Physical Security Review Committee.

PART II - CLASSIFICATION MANAGEMENT

2-1 Classification

1. Basic Policy. Information which requires protection against unauthorized disclosure in the interest of national security must be classified as outlined in reference (a). Only three designations are used to denote levels of classification: Top Secret, Secret, and Confidential. Terms such as "For Official Use Only" and "Limited Official Use", for example, will not be used solely to identify classified material. Additionally, modifying or combining terms is similarly prohibited, i.e. Secret Sensitive.

2. Original Classification Authority. Commanding Officer, Naval Submarine School, does not have original classification authority and, therefore, may not classify information as Top Secret, Secret, or Confidential. The next senior in Naval Submarine School chain of command with original classification authority (OCA) is Chief of Naval Operations.

3. Classification Guides. As stated above, Naval Submarine School does not originally classify information, but derives information classification from already published sources. Exhibit 2A details which Security Classification Guides are held by Naval Submarine School, and in which departments they are located. A complete list of all Navy classification guides available are listed in enclosure (1) of reference (g).

4. Derivative Classification. Derivative classification is accomplished when anyone incorporates, paraphrases, restates or generates in new form, information which is already classified. Responsibilities of a derivative classifier include respecting original classification decisions, verifying the current level of classification of information insofar as practicable, and carrying forward to any newly created documents previously assigned dates of events for declassification or a notation that the information cannot be automatically declassified without the approval of the originating agency (Originating Agency Determination Required - OADR).

5. Classification Markings. Information from a classified source retains exactly the same markings as those shown on the source material. If a discrepancy regarding classification markings occurs between two separate sources, the appropriate classification guide will provide clarification. DO NOT GUESS.

6. Improper Classification. If substantial reasons exist to believe that information contained in a document is classified improperly, immediately notify the Command Security Manager. If

the document in question is curriculum, the appropriate Course Curriculum Model Manager (CCMM) will be contacted. If Naval Submarine School is the CCMM, and the course was developed by a civilian contractor or command, inform CISO, in addition to the Command Security Manager.

2-2 Marking

1. Basic Policy. All classified material will be marked properly in accordance with reference (a), Chapter 9. This includes any binders in which classified material may be stored, permanent cover sheets, command generated material, or student notes.

2. Requirements. Classified material generally will consist of an unclassified cover page with an unclassified title. Any classified material placed within a folder, binder, or other type of exterior covering designed for classified material must have the highest classification of the document(s) contained within printed clearly on the outside of the binder.

3. Responsibilities. Command generated classified material consists of two general categories: curricula and correspondence (including messages).

a. All classified curricula will be reviewed by CISO prior to "going smooth" to ensure it meets all marking standards for curricula as provided by Chief of Naval Education and Training.

b. The drafter is responsible for ensuring the propriety of the markings on all correspondence. By affixing his/her signature, the releaser or "By direction" signer asserts that all the information contained within the correspondence is correct, and that the correspondence, whether message, memorandum, or letter, is in the proper format and MARKED correctly. In all cases reference (a) will be used as the marking authority. Questions regarding marking command generated material should be directed to the Department Security Assistant. If the Department Security Assistant is unable to help, questions should then be directed to the Command Security Manager.

4. Classified Student Notes. Classified school notes may be forwarded to a student's next command, as authorized by the Commanding Officer on a case-by-case basis. Notes will not be forwarded unless the information is irreplaceable, or unattainable at the next command. The following guidelines apply:

a. Personnel planning to forward notes will prepare a notebook in advance by stamping its pages with the highest

classification of information to be received during the course, and numbering all pages in the following fashion: 1 of 100, 2 of 100, etc. Loose leaf pages retained from class handouts will be included as part of the numbering system. If a fixed paged notebook is used for notes, then a separate binder will be used to contain and number loose leaf handouts. The cover of the notebook will be stamped with the highest classification, and the first page of the notebook will contain the standardized downgrading/declassification markings.

b. A limited amount of unclassified material may be sent with the classified class notes. All other unclassified notes may be treated as professional papers and shipped with household goods.

c. All classified material, whether handouts or personally written notes, is the property of the U. S. government. It may not be removed from Naval Submarine School unless processed through the Classified Material Control Center. Notes will usually be forwarded to the service member's next command via the U.S. Postal System. In circumstances when the gaining command is located on Naval Submarine Base New London or within its environs, the notes may be hand-carried. In these cases, the gaining command will issue the courier authorization and receipt for the material as outlined in Chapter 10 of reference (a). Naval Submarine School personnel will provide a courier briefing as outlined in Chapter 16 of reference (a) and Part 3 of this instruction.

d. Personnel with a delayed arrival at their next command of more than 60 days should give careful consideration to their actual need for the classified material. They must ensure the first command is notified to send the class notes to the next command if their orders are changed after the notes have been sent. If medically held or discharged, that command should be told to destroy notes as they are not required.

EXHIBIT 2A

SECURITY CLASSIFICATION GUIDES HELD AT NAVAL SUBMARINE SCHOOL

OPNAVINST	SUBJECT	CODE
5513.1D	Department of the Navy Security Classification Guides	N12, N2
S5513.5A	Undersea Warfare Programs	N5
S5513.5B	Undersea Warfare Programs	N2, N5, N7
S5513.6C	Communications and Satellite Programs	N2
S5513.7C	Mine Warfare Programs	N2
S5513.8B	Electronic Warfare Programs	N2, N5

PART III - ACCOUNTING AND CONTROL

3-1 Accounting and Control

1. Basic Policy. All classified material arriving at the command will be processed through one of four screening or control points at Naval Submarine School. The Classified Material Control Center (CMCC) is responsible for accounting and control of material classified Confidential and Secret. The Top Secret Control Officer (TSCO) is responsible for accounting and control of all Sensitive Compartmented Information (SCI) The Department Head, Submarine Surveillance Equipment Program (SSEP) is responsible for all classified material received via secure facsimile machine.

2. Control of Top Secret Material. The Top Secret Control Officer (TSCO) is the control point within Naval Submarine School for receipt, routing, transfer or destruction of Top Secret material. All Top Secret material coming into or going out of the command must pass through the Top Secret Control Officer.

a. Receipt. The TSCO will process incoming Top Secret Material and messages as follows:

(1) Page check all incoming and command generated Top Secret material upon initial Receipt. Record the results of the page check on the material.

(2) Sign and return the receipt form to the originator.

(3) Assign a separate Top Secret ACN for each piece of material

(4) Complete and attach a Correspondence/Material Control Form OPNAV 5216/10 for the material.

(5) Complete and attach a Record of Disclosure OPNAV 5511/13 to the material to record the identity of each individual to whom the information is disclosed.

(6) Enter complete identifying information of the material into the command's accountability register. This register will be maintained five years after the documents are transferred, downgraded, or destroyed.

b. Routing. The TSCO will route Top Secret Material as follows:

(1) Determine routing requirements within Naval Submarine School. Ensure hand-to-hand transfer of Top Secret material. Maintain constant surveillance of the material by authorized and properly cleared personnel.

(2) Maintain a continuous chain of receipts using the OPNAV 5216/10. Page Checks are required upon assumption of custody by each recipient for retention and upon return to the TSCO.

c. Destruction. The TSCO will destroy Top Secret Material as follows:

(1) Obtain authorization for destruction from the Commanding Officer.

(2) Complete a Record of Destruction, OPNAV 5511/12, identifying the material to be destroyed and naming two appropriately cleared officials who witness the destruction.

(3) Destruction of Top Secret Material will be assigned only to well-trained personnel possessing a Top Secret clearance. Both witnessing officials will accompany the material to the destruction site and physically monitor the destruction. All witnessing officials must be familiar with the provisions of Chapter 17 of reference (a).

(4) Update the ADP databases with current information regarding the material.

d. Transfer. The TSCO will transfer Top Secret Material as follows:

(1) Assign a Top Secret serial number to all outgoing Top Secret correspondence. Ensure a cover letter is sent with the material for accountability purposes.

(2) Transmit the material via the Defense Courier Service as required by reference (a).

3. Control of Secret Material. The Classified Material Control Center (CMCC) is the control point with Naval Submarine School for incoming and outgoing Secret Material.

a. Receipt. Incoming Secret Material will be processed as follows:

(1) Upon receipt, the classified material control clerk will sign and return the registered mail receipt, examine the material to ensure it is complete, sign the internal receipt, and return the receipt to the originator.

(2) A separate Secret ACN will be assigned to each item of Secret material. Items of Secret material that have multiple copies will have a copy number assigned to each copy (i.e. copy 1 of 25 copies). The Secret ACN and copy number, if appropriate, will be annotated on the front cover of the material and on the title page.

(3) A Correspondence/Material Control Form (OPNAV 5216/10) will be completed and attached to the material. The Secret ACN will be placed on this form. The material will be set aside for the appropriate Department Classified Material custodian (hereafter referred to as custodian) to pick up.

(4) The CMCC will enter identifying data from the control form into the Classified Material Inventory database.

(5) Secret material received by a member of this command which has not been processed through the CMCC and command generated Secret material for use within the command (including Instructor Guides, copies of outgoing correspondence to be retained permanently, and working papers in existence greater than 90 days) will be placed in the Secret control system as follows:

(a) The originator/recipient of the Secret material will deliver the material to the custodian.

(b) The custodian will fill out OPNAV 5216/10 with the exception of the ACN.

(c) The custodian will deliver the material along with the partially completed OPNAV 5216/10 to the CMCC.

(d) The CMCC clerk will assign an ACN, mark the material with the ACN, and obtain the custodian's signature for custody of the material. The material will then be treated in the same manner as material received from any other source.

(6) Large bulk shipments of Secret material can remain where it was delivered if approval is received from the CMCC.

b. Routing. Secret material will be routed as follows:

(1) The material will be held in the CMCC to be distributed to the appropriate department custodian. The custodian will sign the OPNAV 5216/10 when the material is picked up and a copy of this form will be retained in the CMCC.

(2) The custodian will deliver the classified material to their department for internal routing. A copy of the OPNAV 5216/10 with the signature of the individual retaining permanent custody of the information will be maintained by the custodian for inventory purposes. The original OPNAV 5216/10 will be maintained with the material. Note: Multiple copies identified by one ACN are exempt from requiring individual custodian signatures. The original OPNAV 5216/10 will be filed with the department custodian. The Department Custodian will maintain a record of secret material in subcustody.

(3) Each custodian will check with the CMCC daily to determine if there is classified material for their department. All Secret material should be picked up within one working day after placed on accountability.

c. Destruction. Secret material will be destroyed as follows:

(1) Prior to commencing destruction, the custodian will complete a Classified Material Destruction Report (OPNAV 5511/12), listing each document identified for destruction. If an ACN has multiple copies assigned and not all copies are destroyed, the custodian will place the copy number of the material being destroyed on the OPNAV 5511/12 to ensure the ACN remains active.

(2) Authorization for destruction of Secret material will be granted only by the Commanding Officer, Executive Officer, Department Head, or Division Officer. The authorizing official must sign the OPNAV 5511/12 prior to actual destruction and the two witnessing officials will sign after destruction is complete.

(3) Destruction of classified material will be assigned only to well-trained personnel possessing a clearance equal to or greater than the material being destroyed. Of the two witnessing officials, one must be at least an E-5 or GS-5. Both witnessing officials will accompany the material to the destruction site and physically monitor the destruction. All witnessing officials must be familiar with the provisions of Chapter 17 of reference (a).

(4) Custodians will arrange for destruction of material under their purview in accordance with local laws and Naval directives. (i.e. absolutely NO burning or attempted recycling of undestroyed classified material.)

(5) Following destruction, the custodian will forward the Classified Material Destruction Report (OPNAV 5511/12), and

the Correspondence/Material Control Form (OPNAV 5216/10) to the CMCC. The CMCC will update the ADP database and file the OPNAV 5216/10 with the destruction report in the Destruction/Transfer file.

d. Transfer. Secret material will be transferred as follows:

(1) Custodians with Secret material to be transferred will deliver it to the CMCC with the original of the OPNAV 5216/10, two mailing labels, an OPNAV 5511/10 Record of Receipt filled out except for the serial number and registered number, and a signed copy of the transmittal letter for each addressee and/or "copy to" command.

(2) The CMCC will assign classified serial numbers to outgoing correspondence, prepare the material for mailing, and mail the material in accordance with reference (a). One copy of the transmittal letter will be sent to the code to verify transfer and one copy will be placed in the classified correspondence file.

(3) The CMCC will update the ADP database and file their copy of the OPNAV 5216/10 with the original in the Destruction/Transfer file.

(4) The CMCC will send a tracer if a return receipt card is not received within 30 days after the material has been mailed.

(5) Secret Material transferred within the command will be hand carried by appropriately cleared persons possessing a valid courier card. SECRET MATERIAL WILL NEVER BE PLACED IN THE GUARD MAIL SYSTEM.

e. Procedures for use of the Correspondence/Material Control Form, OPNAV 5216/10, to maintain command accountability are provided in Exhibit 3A.

f. Specific delineation of the records required to be kept by the CMCC is provided in Exhibit 3B.

4. Control of Confidential Material

a. Receipt. Incoming Confidential material will be processed as follows:

(1) Upon receipt, the Classified Material Control Clerk will examine the material for completeness, sign the return receipt (if included), and forward it to the originator. The originator, registered number (if applicable), and date originated will be entered into the Confidential Material Control Logs maintained in the CMCC.

(2) The material will be issued to the receiving department. The Department Classified Material Custodian's signature must be legible and the date of pick-up should be entered into the Confidential Material Control Log.

b. Transfer. The CMCC will transfer all Confidential material from the command in accordance with reference (a). Confidential material transferred within the command will be hand carried by appropriately cleared personnel possessing a valid courier card. CONFIDENTIAL MATERIAL WILL NEVER BE PLACED IN THE GUARD MAIL SYSTEM.

c. Destruction. Confidential material will be destroyed in accordance with reference (a). Destruction reports are not required for Confidential material except as noted in paragraph 5 below.

5. Control of Secret and Confidential Instructions. Secret and Confidential instructions and notices will be placed on a Correspondence/Material Control Form (OPNAV 5216/10) and assigned an Accountability Control Number (ACN). A copy of the form will be sent to the Administrative Department, Code N12 for cross-referencing in the command directives file. Secret and Confidential directives that are destroyed must be listed on a destruction report, separate from other material, and a copy of the destruction report forwarded to the CMCC and the Administrative Department.

6. Procedures for Handling Classified Messages. Classified messages are received and transmitted at Naval Submarine School via GateGuard. Word Processing Center (WPC) receives message traffic from the Base Consolidated Telecommunication Center (BCT) each weekday, and transmits outgoing traffic to BCT when workload directs. Specific guidance for operation of the BCT is contained in reference (h).

a. Incoming Message. The CMCC will:

(1) Receive classified traffic from the Word Processing Center on disk for distribution to codes with the capability to process secret information. These disks are classified Secret and handled as such.

(2) Assign ACNs to each message that is kept by the command. It is the code's responsibility to inform the CMCC when a message needs to be kept.

(3) Disks that have been processed by the code will be erased and returned to the Word Processing Center.

b. Outgoing Messages

(1) Outgoing messages are routed to Administrative Services (N12) after approval by the Department Head for transmittal via GateGuard.

(2) Outgoing messages will be generated using Message Traffic Formatter (MTF) and submitted on disk with a hard copy.

(3) The originating department will maintain a file of outgoing classified messages. Secret messages will be assigned an ACN and placed on accountability.

(4) Classified messages will be destroyed in accordance with reference (a).

7. Working Papers. Working papers are documents and material accumulated or created while preparing finished material (i.e., rough drafts, testing material). Classified notes from a training course or conference are considered working papers. When working papers contain classified information, they must be dated when created, marked on each page with the highest classification of any information they contain, protected in accordance with the classification assigned, and destroyed when no longer needed. Working papers must be treated as a finished document and meet the requirements of reference (a) for marking and accountability when they contain Top Secret information, when they are released outside of the command, retained for more than 90 days, or filed permanently.

8. For Official Use Only (FOUO). FOUO is a marking which is placed on documents to alert the holder that they contain information which may be withheld from release under the Freedom of Information Act (FOIA). FOUO is not a security classification. Detailed guidance on handling material marked For Official Use Only is contained in reference (i). The following minimum guidance for handling FOUO material is provided but is not meant to replace the guidance contained in reference (i).

a. Location of Markings. An unclassified document that contains FOUO information shall have FOR OFFICIAL USE ONLY printed in capital letters centered at the bottom on the outside of the front cover, on each page containing FOUO information, and on the outside of the back cover. An unclassified directive will be marked similarly except that each page of the directive will be marked on the top and bottom. Other records such as photographs, film, cassette tapes, etc. shall be marked FOR OFFICIAL USE ONLY so that a recipient or viewer knows the status of the information.

b. Release and Transmission. FOUO information may be disseminated within DON activities and between officials of the DON and contractors who conduct official business for the DON. Recipients shall be made aware of the status of such information,

and transmission shall be by means that precludes unauthorized public disclosure. Transmittal documents shall call attention to the presence of FOUO attachments.

c. Transporting. FOUO shall be transported in a manner that precludes disclosure of contents. FOUO information may be sent via first-class mail, parcel post, or fourth-class mail.

d. Safeguarding. During normal working hours, FOUO information shall be placed in an out-of-sight location of the work area if accessible to non-governmental personnel. At the close of business, FOUO shall be stored to preclude unauthorized access. Unlocked files, desks, or similar containers usually are adequate for this purpose.

e. Disposal. Non-record copies of FOUO material may be destroyed by tearing each copy into pieces to preclude reconstructing, and disposed in regular trash containers.

3-2 PRINTING, REPRODUCTION AND PHOTOGRAPHY

1. Reproduction. Reproduction of classified material on equipment within Naval Submarine School is prohibited except where specifically approved by the Command Security Manager. The following requirements apply:

a. Top Secret information will not be reproduced without the consent of the originating activity or higher authority. Requests for approval to reproduce Top Secret material will be routed via the Top Secret Control Officer.

b. Departments possessing a valid need to reproduce classified material will submit a request to the Command Security Manager asking for authorization to designate a copier for reproduction of classified information. This request will be in writing and contain location of the copier, level of classification to be reproduced, point of contact and sufficient justification. If approved, the Department Head or designated representative will be required to approve each use of the copier for reproduction of classified material. A copy of each request will be kept on file by the Department Security Assistant.

c. Per reference (a), a sign will be displayed prominently on or above the copier stating classification limitations and the approval authority; i.e. Department Head's name.

d. A log will be maintained at the authorized copier in which each piece of classified material reproduced is recorded per subject classification, number of pages, date reproduced, and signature of person making the copies.

e. All Secret material reproduced locally must be taken to the CMCC by the Department Custodian to be placed on accountability control.

f. Reproduction machines will be located in areas that are easily observed to ensure that only authorized copies are being made and the number of copies is kept to a minimum. Areas around the reproduction equipment will be free of wastebaskets, excessive clutter, etc. to ensure that classified material being reproduced is not inadvertently left behind. Before securing the copy machine from classified reproduction, the area will be checked for classified material that may have been left on nearby desks or thrown into wastebaskets.

g. Samples, waste, or overruns resulting from the reproduction process will be safeguarded in accordance with the classification of the information involved. This material will be treated as classified waste and safeguarded until properly destroyed.

h. In the event the machine malfunctions, check to ensure that all copies have been removed. Paper "jammed" in the machine and not usable will be treated as classified waste and safeguarded until properly destroyed.

i. After reproducing classified material, make sure the original and all copies have been removed from the machine. Run a blank piece of paper through copier 5 times to verify.

****Note: Personnel authorized to approve reproduction of classified material have the responsibility to ensure that all reproduction prohibitions are observed and the procedures outlined above are strictly followed.**

2. Printing

a. Printing of classified material is controlled by the Administrative Services Division, Code N12, who will provide a job number. The classified material must be hand delivered to the print shop (NPPSO Groton) and picked up by department personnel authorized a courier card.

3. Photography

a. Taking photographs in areas within Naval Submarine School is forbidden, unless specifically authorized by the Department Head involved (i.e. building dedications, award ceremonies, graduations, etc.) Except in those specific instances, visitors will not be allowed to take photographic equipment into any command building.

b. Requests by other government agencies or contractors to take classified photographs or to film classified material within Naval Submarine School should be brought to the attention of the Public Affairs Officer and the Command Security Manager. Requests should include:

(1) Name of requesting agency

(2) Purpose/Justification

(3) Level of Classification anticipated

(4) Date(s)

(5) Visit request information on person taking pictures

(6) Exactly what is desired to be filmed/ photographed

(7) If contracted, contract number and COR certification of need-to-know, facility clearance level

(8) Concurrence of Department Head involved

c. Those individuals obtaining permission to photograph at Naval Submarine School will be monitored to ensure only the specific areas requested are photographed/filmed. All negatives will be taken to the Classified Material Control Center and transferred as outlined in section 3-1.

d. Permission to photograph or film unclassified material within restricted areas will be granted by the Department Head of the area involved. The photography will be monitored at all times to ensure it remains unclassified.

4. Telecopiers. The telecopier at Naval Submarine School authorized to send and receive classified correspondence is located in Submarine Surveillance Equipment Program (SSEP), Code N7. Contact the SSEP Administrative Office to schedule its use. If an unclassified page of any overall stamped classified document is sent over a telecopier, ensure that the appropriate classification for that page alone is reflected.

3-3 Dissemination of Classified Material Outside NAVSUBSCOL

1. Basic Policy. Naval Submarine School does not have authority to approve dissemination of classified material outside the Department of Defense (DOD). In all cases, strict adherence o the guidelines in reference (a) and other governing instructions referenced therein will occur. Regardless, all requests should be routed through the Command Security Manager for review.

2. Dissemination to Foreign Nationals. Under NO circumstances will Naval Submarine School personnel exceed the authority granted by the Navy Officer of Technology Transfer and Security Assistant (NAVOTTSA). NAVOTTSA will provide a list or body of knowledge that may be provided for every foreign visit or class. Their authority extends to various unclassified information. At times, foreign nationals may request certain information, films, etc. that may be classified. Unless express written consent is provided by NAVOTTSA, these materials may not be provided. The International Military Training Officer (IMTO) serves as the primary point of contact. A file of these authorizations will be maintained by the IMTO for review by the Command Security Manager upon request.

3. Dissemination to DOD Contractors

a. Prior to releasing classified information to a DOD contractor, the provider of the information will verify, through the Command Security Manager and the contractor's COR, that a facility access is on record equal to, or superior to, the classification of the information to be provided.

b. Under no circumstances will classified information be disseminated to contractors without COR verification of need-to-know.

4. Distribution Statements. Command originated classified material may require the addition of a Distribution Statement as a means of limiting dissemination of a classified document. Careful review of Chapter 12 and specifically Exhibit 12B of reference (a) will be made by the drafter prior to determining appropriate statements. When in doubt, refer to the Command Security Manager for guidance.

3-4 Safeguarding

1. Basic Policy. Classified material will be used only where facilities, or other conditions, are adequate to prevent unauthorized persons from gaining access. This also applies to the discussion of classified information.

2. Restricted Areas. Areas within Naval Submarine School facilities which are designated as Level I, Level II, and Level III are listed in reference (j). In all cases, these areas will be marked appropriately and protective measures commensurate with the varying degree of security importance will be in place.

3. Temporary Restricted Areas. Temporary restricted areas are areas within non-restricted buildings where classified material is taught or used on occasion. Instructors and supervisors are responsible for posting restricted area signs when classified material is in use.

4. Care During Working Hours. To the maximum extent possible, when classified material or information is being disseminated every precaution will be taken to prevent unauthorized access to the information. This includes:

a. Classified material will be kept covered at all times when removed from secure storage. The appropriate classified material cover sheet (SF 703, SF 704, or SF 705) shall be used for this purpose.

b. Classified waste material such as preliminary drafts, carbons, etc. will be destroyed immediately. If facilities are not present at the time, the material will be treated as classified waste and will be destroyed at the first opportunity.

c. Classified material being processed on a typewriter or a word processing device will adhere to the following rules:

(1) All ribbons will be removed following use and stored as classified information. Cloth ribbons may be considered unclassified after the upper and lower sections have been cycled through the machine five times in the course of regular typing.

(2) Absolutely no classified information may be placed on the hard drive of a computer unless it is specifically approved for use by the Commanding Officer, and location and an appropriate stowage area have been approved/authorized by the Security Officer and Command Security Manager. Classified information should be placed only on removable floppy disks. These floppy disks shall be treated as classified material and stored appropriately. Floppy disks retained for extended periods of time (over six months) that contain classified material should be processed through the CMCC.

d. Two Person Integrity (TPI). Personnel normally will not be permitted to work alone in areas where Top Secret information or information controlled under Special Access Program procedures is used or stored and is accessible to those employees. Two person integrity does not require that both personnel have the same level of access, and does not apply to those situations where one person with access is left alone for brief periods of time during normal duty hours. However, the two person integrity requirement will be strictly enforced outside of the normal duty hours.

e. After hours study. Students returning to restricted buildings after normal working hours for study must be logged in at the quarterdeck of the building. Prior to the student signing out and leaving the building for the evening, the building Duty Petty Officer or properly cleared individual will check the area where the student was studying to verify that any classified material in use has been properly stowed, and the area is left free of classified material.

5. Security Checks. At the end of each working day, Department Heads will require a security check to make sure all classified material is secured properly. The Activity Security Checklist (SF701), and the Security Container Checklist (SF 702) (where appropriate) will be utilized for this purpose. Procedures for using SF 701 and SF 702 forms are contained in Exhibits 13C and 13E of reference (a). Specific command policy for use of the SF 701 and SF 702 forms is contained in appendix B of reference (j). Security checks will assure that:

a. All classified material is properly stowed.

b. Burn bags are either properly stowed or destroyed.

c. Classified waste, e.g. notes, carbon paper, typewriter ribbons, etc., have been properly stowed or destroyed.

d. Security containers are properly locked with all drawers properly shut. (Rotate the combination lock dial at least four complete times in the same direction when securing container for "older" locks, for digital locks only rotate the dial enough to engage the bolt.)

3-5 Storage of Classified Information

1. Security Containers

a. The Command Security Manager and the Assistant Command Security Manager will collaborate in determining if security containers are appropriate. To ensure proper usage of an expensive and valuable asset, an inventory of all safes will be maintained by the Security Manager and by each Department Security Assistant. Personnel disposing of, or requesting, approved security containers will report this information to the Security Manager who will then match up requests. Due to the scarcity of approved containers, NO approved container will be used for storage of unclassified information.

b. Each Department Security Assistant will ensure that combinations to security containers are changed as required by reference (a) and at an interval not to exceed 13 weeks.

c. The combination to all classified material containers within the department will be maintained by the Command Security Manager utilizing the Security Container Information Form (SF 700). The front of the SF 700 will be completed and the original will be separated from the envelope and attached to the inside of the container. The safe combination will be placed inside the envelope, the envelope will be sealed and stamped with the highest classification of the material within the container.

d. The SF 700 to all security containers will be hand carried to the Classified Material Control Center. The SF 700 for each container will be kept by the Command Security Manager inside a GSA approved security container located on the NAVSUBSCOL Quarterdeck, building 518. The SF 700 to this safe will be kept locked in the key locker on the Quarterdeck. The key locker will also be sealed with a serialized metal ball lock seal.

e. Emergency access to locked department classified material containers during working hours can be obtained by contacting the Command Security Manager or the custodian of the container. Anyone requesting emergency access after working hours must contact the Command Duty Officer or the Department Head involved.

f. The location of each classified material container will remain fixed. Any changes to location of containers shall be authorized in writing by the Command Security Manager and the records updated.

g. NAVSUBSCOL Staff are the only personnel allowed to have combinations to security containers. The number of persons having knowledge of the combination to any security container will be kept to a minimum. Any individual having knowledge of the combination will be listed on the SF 700 or the SF 700 addendum sheet provided as Exhibit 3C.

h. Each container shall have an inventory list of all Secret material stored in the container. Safes shall be numbered and marked according to building number, room number and safe number (448.318.1), and shall be marked with a number to indicate the priority in the event of emergency destruction or evacuation [(1) for confidential, (2) for secret, (3) for top secret, and (4) for S.C.I.]. Numbers shall be stenciled on the front upper drawer of the container whenever possible. Only GSA approved containers are used for the protection of classified material.

2. Vaults and Strongrooms. The vast amount of classified training material held by Naval Submarine School dictates the need for using vaults or strongrooms to provide proper storage. Vaults or strongrooms must be built to the standards of Exhibit 14B of reference (a) and certified in writing by the Command Security Manager. Department Security Assistants are responsible for requesting certification statements and for retaining the original certification once issued.

3-6 Transmission of Classified Material. Classified material from Naval Submarine School will be transmitted in the custody an approved carrier and in accordance with the provisions of Chapter 15 of reference (a). At no time will classified material be transmitted via the guard mail system nor will it be hand-carried by individuals without an appropriate clearance and courier authorization.

3-7 Procedures for Issuing Courier Cards

1. Courier cards will be issued by name only to Classified Material Control Center personnel and to Department Classified Material Custodians and alternates designated by letter. Courier cards will be issued on a case-by-case basis to staff personnel and to students who perform courier duties. Personnel issued courier cards will be provided a briefing on the requirements outlined in Chapter 16 of reference (a) by personnel in the Classified Material Control Center using Exhibit 3D. Acknowledgement of this briefing will be retained for a minimum of 2 years.

2. Requests for additional Courier Cards shall be submitted by the requesting department to the Classified Material Control Center. Requests will contain the name, rank/rate, social security number, work center phone number, and sufficient justification for issue for the prospective courier.

3. A "Bearer" card will be maintained at the NAVSUBSCOL Quarterdeck for use by duty section personnel. When duty section personnel utilize the bearer card, it must be accompanied with written authorization in Exhibit 3E.

4. The CMCC will maintain a log of courier cards issued at NAVSUBSCOL. Courier cards will be issued for not more than one year and valid for CONUS use only.

5. SSEP will issue GENSER courier cards to Groom Team personnel only. These cards will be valid to the PRD of the person issued the card or 3 years, whichever is shorter. SSEP administrative assistant will maintain a log of courier cards issued for SSEP, and the courier briefing statements required in paragraph one. Twice annually SSEP will report all courier cards issued by name and courier card number to the CMCC.

3-8 Hand-carrying Classified Material

1. Only those personnel at Naval Submarine School in possession of a valid Department of Defense Courier Card and the documentation outlined above are authorized to hand-carry classified material between buildings or to other Naval Submarine Base locations.

2. When classified material is being carried within the confines of a Naval Submarine School building or between Naval Submarine School buildings as part of normal duties, individuals will take reasonable precautions to prevent inadvertent disclosure. As a minimum, personnel will cover the information with appropriate classified material cover sheets (SF 703, SF 704, or SF 705). If

transporting classified material between buildings by a means other than walking, the material must be double wrapped (a briefcase may serve as the outer wrapping).

3-9 Hand-carrying Classified Material in a Travel Status

1. Because of the security risk inherent in hand-carrying classified material while in a travel status (less airplane travel), the Commanding Officer, Executive Officer, and Department Heads are the only officials who can authorize hand-carrying information in a travel status and then only when:

a. The classified material is required at the traveler's destination,

b. The classified material is not available at the command to be visited, and

c. Because of time or other constraints, the classified material cannot be transmitted by other authorized means.

2. The Command Security Manager or the Assistant Command Security Manager must be advised whenever anyone in a travel status needs to hand-carry classified material to or from the command. They shall ensure that proper procedures for carrying classified material are followed and that the traveler fully understands his/her responsibility for safeguarding the classified material.

3. The Commanding Officer or person officially designated as "Acting" are the only officials authorized to approve hand-carrying classified information on an aircraft. In addition to the courier card and authorization letter, persons hand-carrying classified information must have a written statement authorizing the transmission typed on official travel orders.

3-10 Visitor Control

1. Basic Policy. The Assistant Command Security Manager is delegated visit approval authority for Naval Submarine School. In order to allow for processing and/or possible rejection of the visitor request, all visit requests should arrive at Naval Submarine School Classified Material Control Center no fewer than five working days prior to the intended visit. Visit requests are not considered valid until approved by the Assistant Command Security Manager.

2. Incoming visit requests

a. Visit requests from other DOD commands are expected to be in accordance with reference (a). Accurate points of contact, clearly defined purpose, and building locations are important for fast and accurate processing and delivery. Visit requests with "Purpose: Training", etc. are inadequate.

b. Visit requests from contractors must have a certified need-to-know required verification from the COR or Contracting Officer in addition to a clearly defined reason for visit and accurate point of contact. Failure to have need-to-know certification can cause delay or rejection of the visit request. All contractor visit requests are required to be in compliance with reference (k).

c. Visit requests will be routed to the affected departments following approval. Quarterdecks should maintain these visit requests for the time period listed on the request. At the expiration of the time period they may be purged as being no longer valid. Command Physical Security Assistants will be responsible for maintaining the quarterdeck files.

d. The master file of approved Visit Requests is located in the Classified Material Control Center.

3. Outgoing visit requests

a. Department Heads delegated "By direction" authority are authorized to sign outgoing visit requests following verification of the security data. Verification of the data can be made using the Versatile Training System (VTS).

b. All outgoing visit requests should arrive at the command to be visited a minimum of five, and preferably ten, working days prior to the visit. All visit requests will be in compliance with reference (a).

3-11 Destruction of Classified Material

1. Classified material may be destroyed only when destruction is authorized by reference (l). All other classified material will be destroyed as soon as it is no longer required and will not be retained for more than five years from the date of origin unless authorized by reference (l) or higher authority. To ensure classified holdings are kept to a minimum, the Command Security Manager will direct each department to designate an annual "Clean Out" day. On the day selected, all departments will devote a portion of that day to destruction of unneeded classified holdings.

2. Department Security Assistants are responsible for training personnel within their department assigned to destruction detail in proper safeguarding of classified material. Personnel assigned must have a clearance at least equal to that of the material being destroyed and will be rotated periodically from that duty.

EXHIBIT 3A

PROCEDURAL GUIDE FOR THE USE OF CORRESPONDENCE MATERIAL CONTROL FORM

1. Correspondence/Material Control Form OPNAV 5216/10 will be used for control, routing, destruction, changes, and transfer of classified material, including messages Secret and above, in this command.

2. Control forms consist of an IBM-size hardcard and 3 legal sized flimsy copies. The general use and distribution of the form and copies are as follows:

a. Hard copy. Hard copy will be retained by the CMCC as a custody record and for original data entry into the ADP database.

b. First flimsy copy will be retained by custodian in the Active Material File.

c. Other flimsy copies will be used for the following purposes:

(1) Destruction reports. Secret material OPNAV 5511/12 (Certificate of Destruction) as required by reference (a).

(2) Reporting changes. To report changes to data previously reported to the CMCC for entry into the ADP database.

(3) Reporting transfers. To report transfers of material to the ADP database.

NOTE: All transfers must be made via the CMCC.

3. Use of the Correspondence/Material Control Form OPNAV 5216/10 for changing data previously entered.

a. To keep the ADP listing current, custodians must inform the CMCC of any changes by entering the information to be changed in the remarks section of OPNAV 5216/10 and delivering the flimsy to the CMCC.

b. Retain one copy and file it with the first flimsy copy in the Custodian Active Material File.

4. Use of Correspondence/Material Control Form OPNAV 5126/10 for transferring material outside the command.

a. Custodians having Secret material to be transferred will complete the remarks section of OPNAV 5216/10 signing, dating, and entering the activity to whom the material is transferred.

b. Place the original form from the Custodian Active Material File in the Custodian's Inactive Material File.

c. One copy will be delivered to the CMCC with the material to be transferred.

d. The CMCC will update the ADP database and file the flimsy copy with the hard copy from the locator file in the Destruction/Transfer file.

e. If material is transferred between departments in Naval Submarine School, the material will be returned first to the CMCC and then subcustodied to the receiving department.

5. Action to be taken on ADP printout for Secret Inventory.

a. Monthly, each custodian will be provided a printout of that Department's Secret inventory.

b. Within 5 working days, the custodian will conduct an audit verifying the inventory against his/her records and report any discrepancies to the CMCC for immediate resolution.

c. Department Heads and custodians are accountable to the Commanding Officer via the Command Security Manager for resolution of the monthly audit.

d. Custodians should make pen and ink changes to their effective monthly inventories as transactions occur to facilitate resolution of new monthly audits.

e. The CMCC and each custodian will retain copies of their inventories for 2 years.

f. Twice annually and upon change of command, a complete Secret inventory shall be performed. All classified material held by the department will be sighted. A report listing discrepancies will be provided to the CMCC for resolution.

EXHIBIT 3B

RECORDS REQUIRED

The following records are required as a minimum. Department Heads may establish any additional records for which they perceive a need.

1. The CMCC will maintain:

a. Secret material Locator File - Hard copies of Secret material control forms filed in ACN sequence by year.

b. Secret Material Destruction/Transfer File - hard copy and signed original of the material control form for material transferred and the hard copy, and copy of Certificate of Destruction (5511/12) for material destroyed. Filed in ACN sequence and retained for 2 years.

c. Incoming Mail Logs - copy of the Transaction Report Summary Log for Confidential material.

d. Copies of all audit and inventory reports. (Previous two years)

e. Receipts for material transferred outside the command.

2. Department Classified Material Custodians will maintain:

a. Active Secret Material File - Original Correspondence/ Material Control Form for all material in their custody. Filed in ACN sequence.

b. Inactive Secret Material File - Flimsy copies of all transactions for material transferred and Certificate of Destruction for material destroyed.

c. Monthly Secret audits - Monthly ADP listings of Secret material subcustodied to them.

d. Copies of all inventory reports. (Previous two years).

EXHIBIT 3C

SF 700 ADDENDUM A

Bldg._____ Room #_____ Code #_____
Container #_____ Date Combination Changed_____

Person's Name	Home Address	Home Phone

(TO BE ATTACHED TO FORM 700)

NAVSUBSCOL 5510.3F/1

EXHIBIT 3D

COURIER AUTHORIZATION BRIEFING

I acknowledge understanding my responsibilities as an official government courier as outlined below:

a. The classified material must be in my physical possession at all times, unless proper storage at a U.S. Government activity or appropriately cleared contractor facility (continental U.S. only) is available. Hand-carrying classified material on trips that involve an overnight stop is not permitted without advance arrangements for proper overnight storage in a government activity or a cleared contractor facility. When I surrender any package containing classified material for temporary storage, I must obtain a receipt signed by an authorized representative of the facility accepting responsibility for safeguarding the package.

b. I may not read, study, display, or use classified material in any manner on a public conveyance or in a public place.

c. When the classified material is carried in a private, public or government conveyance, I will not store it in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod or drop tank. I may not leave classified material unattended under any circumstance.

d. A list of all classified material carried or escorted by me will be maintained by my department. Upon my return, I will account for all classified material or provide a receipt card verifying transfer.

e. Whenever possible, I will return the material to my department by one of the other approved methods of transmission (applies for courier duty leaving confines of NAVSUBASE NLON).

f. When hand-carrying classified material within NAVSUBSCOL facilities, the material must be covered to prevent inadvertent disclosure.

g. When passing through access control points for restricted buildings, I will display my courier card and courier authorization letter (if required) to the watch.

h. If my courier duties require transporting classified material on board commercial aircraft, I will contact the Command Security Manager prior to commencing this travel for further instructions.

Signature	Date	Code

EXHIBIT 3E

MEMORANDUM

From: NAVSUBSCOL CDO
To: Personnel Concerned

Subj: AUTHORIZATION TO HAND-CARRY CLASSIFIED MATERIAL

Ref: (a) OPNAVINST 5510.1H

1. The below named individual is authorized to hand-carry classified material as indicated:

a. Name:_____

b. Social Security Number:_____

c. Rank/Rate:_____

d. Courier Authorization Card Number:_____

e. Destination of Material:_____

f. Date Authorized to Hand Carry Material:_____

g. Description of Material:_____

2. This authorization is made with the understanding that the material con only be carried as prescribed in reference (a) and as outlined above.

_____ _____
Authorized Signature Date

EXHIBIT 3F

I. The purpose of this Exhibit is to establish a guideline for Classified Material Control to amplify the procedures of this instruction and OPNAVINST 5510.1H chapter 10.

II. Department Security Organization

A. Department Classified Material Custodian
   1. Assigned in writing by the Department Head
   2. Works directly for the Department Head
   3. Acts as a liaison between the Classified Material Control Center (CMCC) and their department
   4. Responsible for:
      a. Maintaining records for all classified material in their department
      b. Maintaining and administering the classified material audit and inventory system
      c. Monitoring all destruction of classified material in their department
      d. Transfer of all classified material into or out of their department
      e. Receiving all classified material for their department

B. Assistant Department Classified Material Custodian
   1. Assigned in writing by the Department Head
   2. Should be a Division Classified Material Custodian
   3. Assists the Department Classified Material Custodian in all aspects of their job
   4. Prepared to perform the duties of the Department Classified Material Custodian while they are on leave or TAD

C. Divisional Classified Material Custodian
   1. Assigned in writing by the Department Head
   2. Acts as single point of contact for the Department Classified Material Custodian
   3. Responsible for:
      a. Maintaining records for all classified material in their division
      b. Daily supervision of classified material control within their division
      c. Sub-custody of classified material to end users
      d. Originator of transfer and destruction reports for their division to the Department Classified Material Custodian

III. Receipts

A. All Secret material will be processed through the CMCC for distribution.

1. A 5216/10 will be signed when receiving the material from the CMCC
2. The department custodian will receive the original and one copy of the 5216/10 and the remaining copy will be kept by the CMCC.
3. The department custodian verifies the information on the 5216/10 and ensures that the correct number of copies has been received.
4. If only one copy of the material is received, then one control number will be assigned.
   a. If multiple copies of the same material are received, the material will be assigned one control number and the number of items will be typed in the "number of copies" block of the OPNAV 5216 form.
   b. If a set of books or electronic media is received, where each book or tape is part of a set, but contains different information, each book or tape will receive a separate control number.
   c. Material such as instructor or student guides that have multiple volumes will be assigned one control number and the number of volumes will be typed in the "number of copies" block of the OPNAV 5216 form.
   d. The purpose of the "number of copies" block on the OPNAV 5216 form is to show how many items have the particular control number assigned. It is important not to get the "number of copies" confused with the item titles shown on the OPNAV 5216. The only purpose of the "number of copies" block is to assist personnel conducting inventory in locating the right material and the correct number of copies.
5. The department custodian will determine utilization and subcustody the material to the appropriate division.
6. The department custodian safeguards the material in approved storage containers until picked up by the subcustodian

B. All Confidential material will be processed through the Classified Material Control Center (CMCC) for distribution.

1. Confidential material will be logged in the CMCC and stored for the department custodian until pickup.

2. The department custodian will pick up the material from the CMCC and record it in either a log book or database. If a database program is used, ensure that it is backed up frequently to prevent a total loss of confidential records.

IV. Destruction

A. OPNAV 5511/12 destruction reports will be filled out by the Division Classified Material Custodian

B. Destruction reports will then be signed by the Department Head for authorization to destroy the material

C. Material authorized for destruction will be destroyed within 72 hours of authorization

D. Secret material will be destroyed in accordance with reference (b) Chapter 17 by two individuals with a clearance at least as high as the material to be destroyed. The destruction will be monitored by the Department Classified Material Custodian, and they may be one of the individuals performing the destruction

E. Confidential material will be destroyed in accordance with reference (b) Chapter 17 by at least one individual with a confidential or higher clearance

F. Signature of both individuals indicates actual destruction of the material

G. Destruction reports will be turned in to the CMCC as soon after the destruction as possible to clear the destroyed material out of the database

H. Destruction reports will be retained for two years

V. Transfers

A. OPNAV 5216/158 Routine Reply form or OPNAV 5511/10 will be filled out by the Division Classified Material Custodian

B. The transfer form will then be signed by the Department Head for authorization to transfer the material

C. The material authorized for transfer and the transfer form will be delivered to the Classified Material Control Center by the Department Classified Material Custodian

D. The Department Classified Material Custodian will insure that the material is transferred from their department in the database

E. Transfer forms will be retained for two years

VI. Working Papers

A. When working papers contain classified information, they must be dated when created, marked on each page with the highest classification of any information they contain, and protected in accordance with the assigned classification.

B. Any secret material generated that will be held for 90 days or more will be placed into the classified material control system. This includes:
   1. Instructor guides
   2. Student notes for classes longer than 90 days

C. All computer disks containing secret information will be placed in the classified material control system. There is no such thing as a secret working disk.

VII. Records

A. A copy of the OPNAV 5216/10 will be kept on file at the CMCC. The original of the form will be kept by the Department Classified Material Custodian. The second copy will be held by the Division Classified Material Custodian the material is subcustodied to. This last copy is to be kept with the material if practical.

VIII. Audits and Inventories

A. Department Classified Material Custodians will establish an audit/inventory system to include inventories conducted at each of the following events:
   1. Change of Command
   2. Change of Department or Division Classified Material Custodian
   3. Change of Department Head
   4. If any of the above circumstances does not occur within any six month period an inventory of classified material will be conducted. The purpose of this system is to conduct an inventory at least every six months.

B. Inventories will check for the following:
   1. Discrepancies between the audit list supplied by the CMCC and the material on hand. These will be reported to the CMCC for action.
   2. Material that is no longer needed and can be marked for destruction
   3. Material that can be downgraded to a lower classification

C. Inventory procedure:
   1. All materials will be sighted for the inventory
   2. Generate a list of materials in each container
   3. Compare the list of materials to the audit list supplied by the CMCC
   4. Generate a list of discrepancies and forward to the library

D. The Assistant Security Manager and Security Officer will perform random spot checks of all departments

E. Inventory results will be reported to the responsible Department Head immediately upon completion. Results will then be forwarded to the CMCC

F. Results of inventories will be retained for two years

PART IV - PERSONNEL SECURITY CLEARANCES

4-1 Basic Policy. All staff and student personnel at Naval Submarine School must maintain a clearance and access at a level required for the performance of their duties. While at the command an individual may be required by message, etc, to submit an investigation. The individual is responsible to provide all information in a timely manner. Lack of submission of appropriate investigation forms could result in the inability of the member to perform his/her assigned tasks.

4-2 Staff Check-in

1. All personnel, whether assigned to a billet that requires access to classified material or not, are required to check into the Classified Material Control Center (CMCC) with the Assistant Command Security Manager. New arrivals must have their NAVSUBSCOL 5520/1 filled out prior to check-in indicating the required level of access. Personnel requiring access to Sensitive Compartmented Information (SCI) will check in with the Special Security Officer in Building 448.

2. When access is required, the CMCC will place the member in an interim status, grant access, and submit the appropriate adjudication paperwork to the Department of the Navy Central Adjudication Facility (DONCAF). The CMCC will annotate the Certificate of Personnel Security Investigation, Clearance and Access (OPNAV 5520/20) and enter the clearance information in the Versatile Training System (VTS). Unless unusual circumstances exist, personnel checking into NAVSUBSCOL without a valid investigation will not be granted an interim clearance until a request for an investigation has been submitted.

3. When message confirmation from DONCAF is received authorizing a final clearance on a service member, the CMCC will place the message in the service member's field service record and the VTS will be updated. No additional entries on the OPNAV 5520/20 will be made.

4-3 Expired Top Secret Access

1. Staff members already at NAVSUBSCOL will be notified in writing six months prior to investigation expiration of the requirements for submission of a periodic review, and shall be given ONE MONTH to prepare the paperwork. Failure to complete the appropriate investigation forms could result in the administrative removal of access and the inability of the member to perform his/her assigned tasks.

2. Additionally, personnel who are required to maintain continuous eligibility for Top Secret and Secret access are listed by both rate and position in Chapter 21 of reference (a). These personnel also will be required to submit a Personnel Security Questionnaire for an SSBI regardless of whether they have or need a current access to Top Secret (or other types of information).

4-4 Submission of Investigation Paperwork

1. Required forms for all investigations will be supplied by the Personnel Security Investigations Center to personnel requiring an initial investigation (SSBI) or update (SSBI-PR). SSBI paperwork for SCI access will be supplied to selected individuals by the Special Security Officer.

2. All members are responsible for neatly printing all the information required on the forms. The directions provided with the forms must be followed strictly and any information not readily available (zip codes, past supervisor's phone number, etc.) must be researched thoroughly by the individual prior to submission. Upon completion of the forms, the individual will submit them to the Personnel Security Investigations Supervisor for review. The Personnel Security Investigations Division will type the forms, take the individual's fingerprints, and forward the forms per reference (a).

3. All personnel ignoring two requests for submission of a new investigation package, due to the expiration of a previous investigation or the need for an original investigation for clearance eligibility, are subject to downgrading of access and loss of security clearance eligibility.

4. Follow-up action on clearance requests, i.e., correction of forms, submission of notice of cancellation, submission of tracer action for undue delay, etc., will be the responsibility of the Personnel Security Investigation Supervisor.

4-5 Student Clearances. Due to the unique nature of Naval Submarine School, most of the clearances required for students who are new accessions are submitted by this command. It is, therefore, extremely important that all students, officer and enlisted, complete required investigation packages in a timely manner. A delay in submission of a security investigation could result in the individual's inability to perform assigned duties at his/her next command or in the delay of transfer.

4-6 Intra-Command/Department Transfers. Occasionally transfers will occur between departments or within a department which require a member's clearance/access to be either upgraded or downgraded. If this occurs, the member must report to the

Assistant Security Manager with a memorandum from the new division or department director indicating a new clearance is required.

4-7 Continuous Evaluation for Eligibility

1. All members of the command, particularly those in personnel, security, legal and supervisory positions must report any unfavorable information obtained or developed which places a member's ability to safeguard classified information in question. Co-workers have an equal obligation to advise their supervisor, department security assistant, etc., when they become aware of information with potential serious security significance regarding someone with access to classified information. Exhibit 4A contains a list of behaviors which may render one ineligible for continued assignment in a position of trust.

2. When potentially harmful information is acquired about an individual with a security clearance, the Command Security Manager will be notified in order to alert DONCAF. The information will be forwarded to DONCAF using a Personnel Security Action Request (OPNAV 5510/413) for consideration and adjudication.

4-8 Revocation of Clearance/Access. The revocation or denial of security clearance/access only can be accomplished by the DONCAF. DONCAF can issue letters of intent to deny or revoke security clearance eligibility based upon the results of a security investigation or information received by law enforcement or command authorities. A member who has demonstrated high risk behavior exposes himself/herself to blackmail and will not be placed in a position that can be exploited or possibly cause serious damage to the nation. Persons in receipt of a "Letter of Intent to Deny/Revoke Security Clearance Eligibility" from DONCAF will be notified by the Personnel Security Investigations Supervisor who will provide information on options available to the service member.

4-9 Administrative Downgrading of Clearance/Access

1. The administrative downgrading of clearance and access is a non-punitive action and has no long term effect on a service member's career. Administrative downgrading of clearances shall occur when:

a. Member is transferred to a billet which requires a lower clearance or no access to classified information.

b. Member is processed for discharge.

c. Staff member is in a UA status for more then 24 hours or a student is in a UA status for more than 5 days.

d. Member has pending legal problems of a significant nature.

2. The Legal Officer must inform the Command Security Manager or Personnel Security Investigations Supervisor of all cases which fall under his/her cognizance regarding punitive/other than honorable discharges, unauthorized absentees, and significant military, medical, or legal problems. The Student Control Officer should inform the Command Security Manager of all personnel being processed for discharge, being dropped as academic attrites or for medical reasons. Personnel making interdepartmental transfers shall inform the Command Security Manager of any necessary lowering or upgrading of clearances within two days of the transfer.

** **EVERY EFFORT MUST BE MADE TO ELIMINATE UNNECESSARY SECURITY CLEARANCE REQUESTS, CANCEL REQUESTS THAT ARE NO LONGER APPROPRIATE, AND AID IN LESSENING INVESTIGATION RUN TIME.**

EXHIBIT 4A

SIGNIFICANT PERSONNEL SECURITY FACTORS

1. The following are considered significant personnel security factors:

a. Incidents, infractions, offenses, charges, citations, arrests, suspicion or allegations of illegal use or abuse of drugs or alcohol, theft or dishonesty, lack of reliability, irresponsibility, immaturity, instability or recklessness, the use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions.

b. All indications of moral turpitude, sexual promiscuity, heterosexual promiscuity, aberrant, deviant, or bizarre sexual conduct or behavior, transvestitism, transsexualism, indecent exposure, rape, contributing to the delinquency of a minor, child molestation, spouse-swapping, window peeping, and similar situations from whatever source. Unlisted full-time employment or education; full-time education or employment that cannot be verified by any reference or record source or that contains indications of falsified education or employment experience. Records or testimony of employment, education, or military service where the individual was involved in serious offenses or incidents that would reflect adversely on the honesty, reliability, trustworthiness, or stability of the individual.

c. Mental, nervous, emotional, psychological, psychiatric, or character disorders/behavior or treatment reported or alleged from any source.

d. Excessive indebtedness, bad checks, financial difficulties or irresponsibility, unexplained affluence, bankruptcy, or evidence of living beyond the individual's means.

e. Any other significant information relating to the criteria included in paragraph 22-2 of OPNAVINST 5510.1H.

2. Any of the above information developed concerning an individual affiliated with the Department of the Navy is to be reported to DONCAF with all pertinent information and any action taken by the command.

NAVSUBSCOL INSTRUCTION 5510.3F CHANGE TRANSMITTAL ONE

Subj: COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM

Encl: (1) Revised Exhibit 2A

1. Purpose. To promulgate Change One to the basic instruction.

2. Action. Make the following pen and ink changes.

a. Page i, Table of Contents, change "Automated Information System Security Officer" to "Information Security Officer".

b. Page 1-1, paragraph 4., change "department" to "director" throughout the paragraph.

c. Page 1-2, paragraph 4., change "department's" to "directorate's".

d. Page 1-2, paragraph 4.c., change "Chief Master at Arms" to "Physical Security Officer".

e. Page 1-2, delete paragraphs 4.e and 4.f.

f. Reletter paragraph 4.g. to 4.e.

g. Page 1-2, paragraph 4.e, change "Department" to "Command"; "Assistant" to "Assistants" and "Automated Data Processing Security Officers" to "Information Security Officers".

h. Page 1-3, paragraph 5.c., change "Secret" to "secret".

i. Page 1-3, paragraph 7, change "Automated Data Processing Security Officer (ADPSO)" to "Information Security Officer (ISO)." Change "ADPSO" to "ISO".

j. Page 1-3, paragraph 8., add "Security Officer," before Executive Officer.

k. Page 1-6, delete paragraph 7 and renumber paragraph 8 accordingly.

l. Page 1-7, paragraph 4., change "Chief Master at Arms (CMAA)" to "Command Quarterdeck" and add "Command Duty Officer," before Command Security Manager. Second sentence delete "or CMAA".

m. Page 1-7, paragraph 5.b., delete "the Director, Security Department".

n. Page 1-9 delete paragraph 1.d.

o. Page A1-2, paragraph 5.a(4), change "the" to "their".

p. Page A2-1, change Department Security Assistant to "Directorate Security Assistant".

q. Page A2-2, delete the first paragraph.

r. Page 2-2, paragraph 3.a., delete "Chief of Naval Technical Training and".

s. Page 3-6, paragraph 5., change "Code 021" to "Code N12".

t. Page 3-7, paragraph 6.1.(3), change to read: "Assign a separate ACN to each Secret message".

u. Page 3-7, delete paragraph 6.b.(2) and renumber the following paragraph accordingly.

v. Page 3-9, Section 3-2, paragraph 1, delete "Department".

w. Page 3-9, Section 3-2, paragraph 1.c., delete "Department".

x. Page 3-10, paragraph 2.a. change "Code 021" to "N12", and change the last sentence to read, "and picked up by Security Department personnel".

y. Page 3-10, delete paragraph 2.b.

aa. Page 3-11, paragraph 3.b.(7), change "COTR's" to "COR's".

bb. Page 3-11, paragraph 4., change "05" to "N7".

cc. Page 3-12, paragraphs 3.a. and 3.b., change "COTR" TO "COR".

dd. Page 3-14, paragraph 4.e., change "Duty Master at Arms" to "Building DPO".

ee. Page 3-15, para 1.a. change, "Security Officer" to "Security Manager".

ff. Page 3-15, paragraphs 1.c, 1.d., and 1.e., change "Department Security Assistant" to "Command Security Manager".

gg. Page 3-15, paragraph 1.f, change to read: "The location of each classified material container will remain fixed unless the Command Security Manager is notified in writing and the required records are updated".

hh. Page 3-16, Section 3-7, paragraph 2.: insert the word "sufficient" just before the word "justification".

ii. Page 3-16, Section 3-7, paragraph 3., change the third sentence to read: "These courier cards will be issued to personnel performing courier duties by the Directorate Classified Material Custodians".

jj. Page 3-17, paragraph 5., change "Department Security Assistant" to "Directorate Classified Material Custodian".

kk. Page 3-18, Section 3-10, paragraph 2.b., change "COTR" to "COR".

ll. Page 3-19, paragraph c., change "Department" to "Command".

mm. Page 3A-3, change "Via" to "Director, Code _____"; in the From: line in the endorsement and the signature line delete the word "Department".

nn. Page 3E-1, delete the word "Department" in the From line.

oo. Remove Exhibit 2A from the instruction and replace it with enclosure (1) to this change transmittal.

pp. Annotate the first page of the basic instruction, upper right hand corner CH-1 entered __date__ by __initials__.

J. C. BRANDES

Distribution:
Case A

NAVSUBSCOL INSTRUCTION 5510.3F CHANGE TRANSMITTAL TWO

Subj: COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM

Encl: (1) Pages 1-1 through 1-5
(2) Pages A2-1 and A2-2
(3) Pages A5-1 and A5-2
(4) Pages 3-17 and 3-18
(5) Exhibit 3E

1. Purpose. To promulgate Change Two to the basic instruction.

2. Action. Make the following pen and ink changes.

a. First page, under reference list, add "(m) NAVSUBSCOLINST 5239.3A".

b. On page i, change "TABLE OF CONTECTS" to "TABLE OF CONTENTS".

c. Make the following changes to TABLE OF CONTENTS, PART I:

(1) Under 1-1, line 1., change "Director" to "Department Head".

(2) Under 1-1, line 5., change "1-3" to "1-2".

(3) Under 1-1, line 7., change to read "Automated Information System Security Officer".

(4) Under 1-3, change "1-4" to "1-5".

(5) Under 1-4, line 1., change "Purpose" to "Basic Policy".

(6) Under 1-4, line 7., delete complete line and change number "8" to "7".

(7) Under Appendixes, add new "Appendix (5) - Command Security Manager/Security Officer..A5-1"".

d. Make the following changes to PART I - PROGRAM MANAGE-MENT:

(1) Remove pages 1-1 through 1-5 of basic instruction and replace with enclosure (1) of this change transmittal.

(2) Section 1-5, paragraph 5.b., after "Command Security Manager," add "Legal Officer".

e. Make the following changes to Appendix 1:

(1) Paragraph 5.a.(4), change "director" to "head".

(2) In paragraphs 5.d.(1), 5.d.(2) and 5.e.(2), change "Department Director" to "Department Head".

f. Remove pages A2-1 and A2-2 of basic instruction and replace with enclosure (2) of this change transmittal.

g. Remove pages A5-1 and A5-2 of basic instruction and replace with enclosure (2) of this change transmittal.

h. Make the following changes to PART III - ACCOUNTING AND CONTROL:

(1) Section 3-1, paragraph 1., change "Director" to "Department Head".

(2) Section 3-1, paragraph 3.b.(2), add "The Department Custodian will maintain a record of secret material in subcustody."

(3) Section 3-1, paragraph 3.c.(2), delete "or Department Head" and add "Department Head, or Division Officer".

(4) Section 3-2, paragraph 1., delete "Director, Executive Officer or Commanding Officer".

(5) Section 3-2, paragraph 1.b., change "Director" to "Head".

(6) Section 3-2, paragraph 1.c., change "Director's" to "Department Head's".

(7) Section 3-2, paragraphs 1.g. and 1.h., change "destroyed properly." to read "properly destroyed."

(8) Section 3-2, paragraph 1.i., after "through copier" add "5 times".

(9) Section 3-2, paragraphs 3.a., 3.b.(8), and 3.d., change "director" to "head".

(10) Section 3-3, paragraphs 3.a. and 3.b., change "COTR" to "COR".

(11) Section 3-4, paragraph 4.c.(2)., after "Commanding Officer," change to read "and location and an appropriate stowage area has been approved/authorized by the Security Officer...".

(12) Section 3-4, paragraph 4.e., change "stored properly" to "properly stowed".

(13) Section 3-4, paragraph 5., change "Director" to "Head" and "stored properly" to "properly stowed".

(13) Section 3-4, paragraphs 5.a., 5.b., and 5.c., change "stored properly" to "properly stowed".

(14) Section 3-4, paragraph 5.d., delete contents in parentheses and add "(When securing container, rotate the combination lock dial: a) for S&G lock at least four complete turns in one direction or b) for XO7 lock turn the dial far enough to engage bolt.)"

(15) Section 3-5, paragraph 1.b., after "reference (a)," add "and at an interval not to exceed 13 weeks,".

(16) Section 3-5, paragraph 1.e., change "Director" to "Head".

(17) Section 3-5, paragraph 1.f., change paragraph to read: "The location of each classified material container will remain fixed. Any changes to containers shall be authorized in writing by the Command Security Manager and the records updated."

(18) Section 3-5, paragraph 1.g., at the end of first sentence add "SUBSCOL Staff only."

(19) Section 3-7, paragraph 1., at the end of first sentence add "designated by letter."

(20) Section 3-7, paragraph 2., delete "personalized".

(21) Section 3-7, paragraph 3., delete entire paragraph and replace with: "A "Bearer" card will be maintained at the SUBSCOL quarterdeck for use by duty section personnel. When duty section personnel utilize the bearer card, it must be accompanied with written authorization in Exhibit 3E."

(22) Remove pages 3-17 and 3-18 of basic instruction and replace with enclosure (4) of this change transmittal.

(23) Section 3-10, paragraph 2.c., change "Department Security Assistants" to "Command Physical Security Assistants".

(24) Section 3-10, paragraph 3.a., change "Directors" to "Heads".

i. Make the following changes to Exhibit 3A:

(1) Paragraph 5.b., delete "(use the Sample Letter of Resolution of Monthly Audit as a guide)".

(2) Paragraph 5.c., after "Commanding Officer" add " via the Command Security Manager,".

(3) Paragraph 5.e., delete "monthly audits and" and change "1 year." to "two years."

(4) Paragraph 5.f., first sentence, change "At least" to "Twice".

(5) Delete page 3A-3.

j. Make the following changes to Exhibit 3B:

(1) Delete paragraph 1.d. and reletter remaining sub-paragraphs.

(2) Paragraph 1.d., change "one year" to "two years".

(3) Paragraph 2.d., delete "audit and" and change "one year" to "two years".

k. Remove Exhibit 3E of basic instruction and replace with enclosure (5) of this change transmittal.

l. Make the following changes to PART IV - PERSONNEL SECURITY CLEARANCES:

(1) Section 4-3, delete paragraph 1. and renumber remaining paragraphs.

(2) Section 4-4, paragraph 1., delete "a five year".

m. Annotate the first page in the upper right hand corner with CH-1 entered (date) by (initials).

JOHN C. BRANDES

Distribution:
Case A

NAVSUBSCOLINST 5510.3F CH-3
01E
2 Apr 97

NAVSUBSCOL INSTRUCTION 5510.3F CHANGE TRANSMITTAL THREE

Subj: COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM

Encl: (1) Table of Contents
(2) Part III
(3) Exhibits 3A through 3F

1. Purpose. To promulgate Change Three to the basic instruction.

2. Action. Make the following pen and ink changes.

a. Remove Table of Contents from basic instruction and replace it with enclosure (1) of this change transmittal.

b. Remove Part III from basic instruction and replace it with enclosure (2) of this change transmittal.

c. Remove Exhibits 3A through 3F from basic instruction and replace them with enclosure (3) of this change transmittal

d. Annotate the first page in the upper right hand corner with CH-3 entered (date) by (initials).

JOHN C. BRANDES

Distribution:
Case A

NAVSUBSCOLINST 5510.3F CH-4
01E
24 Jun 98

NAVSUBSCOL INSTRUCTION 5510.3F CHANGE TRANSMITTAL FOUR

Subj: COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM

Encl: (1) Revised paragraph 8 and new paragraph 9 of Part I
(2) Revised paragraph 6 of Part III

1. Purpose. To promulgate Change Four to the basic instruction.

2. Action. Make the following pen and ink changes.

a. Part I, delete paragraph 8 and replace with enclosure (1) of this change transmittal. Renumber remaining paragraphs "9 and 10" to "10 and 11".

b. Part I, delete section "1-3 Inspections and Review" in its entirety. Renumber all remaining sections.

c. Part I, section 1-3, first line, remove the word "ass".

d. Part III, remove paragraph 6 and replace with enclosure (2) of this change transmittal.

e. Exhibit 3F, Part VIII., A., delete line 4, renumber line "5" to "4".

f. Annotate the first page, upper right hand corner of basic instruction with "CH-4 entered (date) by (initials)."

K. B. LEAHY

Distribution:
Bulletin Board